AFFIDAVIT IN SUPPORT OF
AN APPLICATION

AFFIDAVIT

I, Carol-Anne Dowling, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation and have been since December 4, 2022. I am currently assigned to the Phoenix Division - Tucson Resident Agency, Complex Financial Crimes Squad and was previously assigned with the Public Corruption Squad. Prior to being a Special Agent with the FBI, I worked in education for nine years. As a Special Agent in the FBI, I have received training at the FBI Academy located in Quantico, Virginia. I have received additional training in the identification and enforcement of laws of the United States and the State of Arizona. I have, through training and experience, become familiar with and used normal methods of investigation, including, but not limited to, visual surveillance, interviewing witnesses, victims, and subjects, subpoenas, search and arrest warrants, confidential human sources, and court authorized wiretaps. In addition, through training and experience, I have become familiar with the manner in which electronic devices, including cellular telephones, may be used in the furtherance of criminal activity, and how information from these devices may be stored, collected, and reviewed in order to obtain evidence of criminal activity.

2. This affidavit is made in support of an application for a warrant to search a white Apple iPhone, ("**Subject Phone 2**"), and a blue OnePlus Android ("**Subject Phone 3**") (collectively, the "**Subject Phone**s") described further in Attachment A1 and A2, for evidence, instrumentalities, and contraband described further in Attachment B, concerning conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, and conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h) (collectively, the "Subject Offenses").

3. On or about November 20, 2024, United States Court for the District of Arizona Magistrate Judge Maria Aguilera signed a criminal complaint and arrest warrant authorizing the arrest of Ahmed Maqbul Syed ("SYED") and a co-conspirator Rupesh Chandra Chintakindi ("RUPESH") for violations of the Subject Offenses in 24-05345-MJ-LCK.[1] On December 11, 2024, RUPESH and SYED were indicted in the District of Arizona, Tucson division in CR24-08825-TUC-JCH (LCK). SYED was indicted with Conspiracy to Commit Wire Fraud and Conspiracy to Commit Money Laundering. RUPESH was indicted with Conspiracy to Commit Money Laundering. The general nature of the scheme against these defendants is as follows:

4. Various elderly victims around the United States to include multiple victims in Arizona were defrauded in what is commonly referred to as a "tech support," "business imposter," and "government imposter," scheme. Generally, some victims received a "pop up" on their electronic device that froze the device. Victims were also directed to contact "tech support" or "government representatives" – in reality, the victims were directed to other scam operators who further developed the fraudulent scheme. Unbeknownst to the victims, the individuals the victims contacted were part of the scam. The scammers informed the victims their accounts had been hacked and compromised. The victims were directed to withdraw and transfer money and cash to protect their accounts. Victims were also directed to purchase gold and that individuals would retrieve the gold from the

[1] The facts outlined in the criminal complaint contained several inadvertent misstatements of fact to include that the Fayez corporation bank account was a joint account held by SYED and an individual believed to be his wife. However, the defendant's wife was the only person who had signature authority on this account. Further, the complaint incorrectly alleged that communications between SYED and RUPESH were collected from both of their phones. These communications were only collected from RUPESH's phones. These factual discrepancies were not material to the probable cause alleged in the complaint.

victims. An example of how the scheme operated is detailed below relating to Marana, Arizona victim M.D. who lost over $700,000 because of the scam.

Marana, Arizona Victim M.D. (Approximate Loss = $770,000)

5. On February 10, 2024, M.D.'s iPad froze when an alert "popped up" on her screen. M.D. was directed to contact technical support for what M.D. was led to believe was the computer company Apple. After contacting the number, M.D. was told that her computer had been hacked and they were using it for child porn and gambling. The scammer directed M.D. to contact whom she was led to believe was a representative from the Federal Trade Commission (FTC) to make a report. After contacting this individual, the scammer informed M.D. that her accounts were at risk. The scammer further stated that he would help protect M.D.'s money. The scammer also directed M.D. to move her money from her investment accounts (Fidelity) to her checking account. The scammer ("Andrew Katsaros") told M.D. the amount to transfer so that she would not have to obtain approvals from Fidelity for the transfers. M.D. was told she would receive a check from the U.S. government once they received her assets. M.D. made various electronic transfers of her funds from her investment account at Fidelity to her personal checking account with Chase Bank to include the following transfers:

2/26/24 electronic transfer for $90,000

3/08/24 electronic transfer for $100,000

3/12/24 electronic transfer for $90,000

3/15/24 electronic transfer for $90,000

3/28/24 electronic transfer for $90,000

4/2/24 electronic transfer for $100,000

4/3/24 electronic transfer for $100,000

4/12/24 electronic transfer for $25,318.33

6. The instructions to help complete each of the above electronic transfers were transmitted through a server located outside of Arizona. On or about February 23, 2024, the scammer instructed M.D. to withdraw $30,000 in cash from her account, wrap the money in a paper bag and wait for an agent to retrieve the funds. M.D. did as she had been instructed. A male arrived at her home and provided her with a password to retrieve the money. M.D. provided the cash to the individual who left on foot.

7. Between February 27, 2024, and April 22, 2024, M.D. received instructions to purchase gold in varying amounts to further protect her money. On or about February 27, 2024, M.D. initiated a wire transfer for $107,886.08 from her Chase bank account ending in 2308 using proceeds from the $90,000 February 26, 2024, electronic transfer into M.D.'s account from Fidelity. As instructed, M.D. used these funds to purchase gold bars from an online gold dealer. The gold was mailed to the victim via FedEx. M.D. was directed to meet at the Walgreens on Dove Mountain Blvd. in Marana, AZ to deliver the gold. After arriving at this location, she observed the vehicle that would receive the gold. M.D. provided the gold through the rear passenger window of this vehicle. After receiving the gold, the male drove the vehicle away.

8. M.D. received additional instructions for the purchase and delivery of gold. M.D. conducted additional purchases of gold from various gold dealers. On March 18, 2024, M.D. purchased approximately $281,000 in gold bars. On April 4, 2024, M.D. purchased approximately $352,000 in gold bars. Both these purchases were made using mostly the proceeds from the above electronic transfers from M.D.'s Fidelity investment account to her Chase bank account. These orders were also delivered to M.D. via FedEx. M.D. received additional instructions for the delivery of these gold purchases and provided the

gold to an individual she met at the same Walgreens parking lot. M.D. made each of the above transfers of gold to an individual M.D. described as a white male, age 30-35 years old.

9. On or about April 16, 2024, M.D. cashed out her $500,000 Pacific Life Insurance life insurance policy and caused those funds to be electronically transferred into her Chase bank account. Per a representative of Pacific Life, their servers relating to this transfer are in California. On April 22, 2024, M.D. attempted to place an order for $251,000 in gold bars. She went to Chase Bank to purchase gold bars. Chase Bank told her that she should not purchase any more gold bars unless she goes to a reputable dealer because they believed she was being scammed. M.D was referred to Precious Metals Refinery to purchase the gold bars. M.D. contacted the Marana, Arizona Police.

10. During the scheme, M.D. stated that she was in constant contact with the person she believed was "Andrew" through text message and phone calls. M.D. was told to maintain her privacy and not speak about the case.

MAY 2, 2024 – CONTROLLED DELIVERY

11. M.D. purchased a package of gold from Precious Metals Refinery in Marana, Arizona. Marana, Arizona Police engaged in a controlled delivery to attempt to apprehend the courier. M.D. then returned to her home. Real gold was not used during the controlled delivery – but the box she received from the gold dealer was used as a decoy package. M.D. received instructions from the scammer over the phone concerning how the delivery would be made. The subject (who claimed to be Andrew from the Federal Trade Commission) stated that one of his agents would collect the package. M.D. was instructed to remain on the phone until the delivery was done. M.D. was instructed to drive to the main gate of her community. During that time while near her residence, M.D. met the driver of a Nissan Altima who was supposed to retrieve the package. M.D.

exited her vehicle and placed the package in the passenger side of the Altima. M.D. stated that she had not seen this driver before. M.D. further stated the driver gave her a password when they met but they did not speak further. Subsequently, officers conducted a traffic stop of the driver, later identified as defendant RUPESH, and took him into custody.

12. Inside of the vehicle RUPESH was driving (rental car), Marana PD discovered 46 one-ounce gold bars wrapped in black socks, inside the trunk and under the spare tire. Further investigation linked this gold to another elderly victim (M.P.) from Scottsdale, AZ (See below). On May 1, 2024, M.P.'s address was texted to RUPESH from "OWEN," an individual law enforcement believe is a fellow unidentified co-conspirator saved under RUPESH's phone under the contact name "OW." M.P.'s receipt for the purchase of gold, dated May 1, 2024, the day before, was also consistent with the type and amount of gold (46 one-ounce bars) found in RUPESH's rental car.[2]

Scottsdale, AZ Victim M.P. – Financial Loss Approximately $209,000[3]

13. Between April 25, 2024, and May 7, 2024, M.P. lost approximately $209,000 through the tech support pop-up scam. M.P. was working on his computer when it froze. A pop-up advised him to contact "Microsoft." After making the call, M.P. was also referred to the "FTC" after being informed M.P. was a victim of identity theft. Upon calling who M.P. believed was the "FTC," M.P. was told that to secure his bank

[2] RUPESH was charged by the Pima County, Arizona attorney's office in State court for his involvement relating to victim M.D. RUPESH fled the country on or about November 4, 2024 while on pretrial release for his State case.

[3] This amount of loss also includes the 46 ounces of gold bars currently in the possession of the Marana Police Department that is expected to be returned to the victim.

accounts, he needed to withdraw money and deposit the funds into bitcoin ATM machines.

14. M.P. made various deposits into Bitcoin ATM machines to include the following:

April 25, 2024 - $20,000 cash

April 26, 2024 - $20,000 cash

These deposits were dispersed to multiple exchanges, including a Bitunex account, which had over $400,000 in the account. The Bitunex account is attributed to a customer in Dubai.

15. M.P. was thereafter directed to purchase gold bars. He purchased 46 ounces of gold from Scottsdale Bullion and Coin on May 1, 2024. M.P. was instructed to send pictures of the gold after he purchased it. The next day, May 2, 2024, MP was instructed concerning the delivery of gold. A Nissan sedan (consistent with the rental car RUPESH was driving) pulled into M.P.'s driveway and rolled down his rear window. M.P. was instructed to place the gold inside the vehicle. M.P. did as instructed.

16. On May 3, 2024, M.P. deposited $20,000 into a Bitcoin ATM.

17. On May 6, 2024, M.P. was advised to withdraw money from his wife's savings account to secure the money in the same manner. M.P. transferred money from his wife's account into his own account. M.P. thereafter withdrew $20,000 and deposited it into a Bitcoin ATM.

18. On May 7, 2024, M.P. made three withdrawals of $6,000, $4,000, $10,000 and deposited this cash into a Bitcoin ATM. Subsequently, M.P. realized he had been scammed and reported the matter to LEO. These deposits were dispersed to multiple exchanges, including a Binance account. The Binance account is attributed to a customer in Dubai.

RUPESH POST-ARREST STATEMENT TO LAW ENFORCEMENT – 5/2/24

19. RUPESH told law enforcement that if he didn't text the people (referring to whom he was working with), they would change everything. He later stated that the people would delete their contacts. RUPESH claimed he was being forced to do this and that hundreds of students were also being forced to do this. RUPESH did not provide any specific details of how he was "forced" other than that the person who hired him would report RUPESH and get him "caught." RUPESH stated that he was a student who had entered the United States from India earlier in the year. While looking for a job, he was referred to an individual RUPESH later described by the nickname "UNCLE" (believed to be SYED). RUPESH was told that he would be doing gold shop deliveries and stated that he never thought it was illegal. After retrieving the first item, RUPESH opened the box and saw gold inside. RUPESH called the person who hired him ("UNCLE") and told him it was illegal. UNCLE told RUPESH it was not illegal. RUPESH provided UNCLE the gold at the gas station. RUPESH claimed he received $200 in return.

20. RUPESH claimed that he had done three deliveries so far. RUPESH further stated he flew to Los Angeles from Chicago. RUPESH also stated they gave him cash and he purchased his plane ticket. RUPESH stated that the main contact was OWEN. The other person is SYED. RUPESH gave varying versions of where he picked up a package or packages going back and forth between Los Angeles and San Francisco. RUPESH stated they give him a phone and change the phone every three days to a week. RUPESH would retrieve the package and photograph the gold and receive a drop off location. RUPESH took a bus to Phoenix where he rented a vehicle. RUPESH also stated they told him to put the 45 or 46 "biscuits" (referring to the gold) in a sock and put it under the tire of the rental car. RUPESH continued to maintain that he picked up the gold that was in his vehicle in Los Angeles. RUPESH was told to pay for everything in cash because if a card was used, all the details would be known. RUPESH also stated that sometimes they

would tell them to retrieve approximately $50,000 or $70,000 of cash and deliver the money somewhere else. However, RUPESH denied retrieving cash. RUPESH claimed he learned about the retrieval of cash from the person at the gas station working with UNCLE.

SEPTEMBER 17, 2024, ARREST OF SYED IN AURORA, ILLINOIS

21. On September 17, 2024, law enforcement executed an arrest warrant on SYED in Aurora, Illinois.[4] A federal search warrant was also executed that day. One of the items searched was SYED's phone. Various communications on RUPESH's phones (two phones – believed to be a burner phone and personal phone) had also been reviewed by law enforcement after his arrest. Evidence recovered on RUPESH's phones, in addition to financial records and other evidence, revealed that SYED and another individual believed to use the name "OWEN" were the individuals who helped coordinate and direct RUPESH relating to the fraud and money laundering conspiracy as reflected by the following examples. Messages between SYED and RUPESH were recovered on RUPESH's personal phone. These same messages were not recovered on SYED's phone. However, it is clear from reviewing the phone evidence that the messages recovered on RUPESH's personal phone were linked to SYED's phone and phone number.

22. On April 11, 2024, RUPESH messaged "Uncle" (SYED) asking if he had "any pickup today, near Milwaukee?" RUPESH also indicated to "Uncle" that he was messaging from his personal phone and he would pick up "another mobile from you" [referring to SYED]. RUPESH further requested the address. Shortly after this request, also on April 11, 2024, SYED messaged RUPESH with an address for Illinois victims

[4] For this arrest, SYED was charged in State court in Indiana relating to his involvement in this conspiracy to an Indiana victim.

B.W. and S.W. The evidence described in this paragraph was obtained from RUPESH's personal phone.

Victims B.W. and S.W. Illinois – Financial Loss approximately $234,000

23. Illinois victims B.W. and S.W. had also been defrauded in this scam out of approximately $234,000. On April 11, 2024, B.W. and S.W. provided $50,000 in cash as they had been instructed. They were told an agent would come by their home to retrieve the package. A black Toyota SUV pulled into the victim's driveway. A female exited the passenger side of the vehicle. She was wearing a wrap around her head and appeared of Iranian decent. She was also on the phone. The female thereafter got back into the vehicle on the passenger side. The victim was instructed to drop the box on the rear passenger side of the vehicle. The victim placed the box in the back seat. The victim observed an elderly Indian male in the back seat. At this time, it is unknown whether RUPESH was the driver of this vehicle. However, this same date, RUPESH received a $500 transfer from Fayez Corporation. The authorized signer on this account was SYED's wife. The following day, RUPESH also messaged SYED a confirmation email dated April 11, 2024, from a hotel that appears to be in Missouri. It is unclear of the date of the hotel stay from this message.

24. On April 22, 2024, RUPESH messaged SYED that he just reached (appearing to refer to the airport) 5 minutes ago and was waiting for a bag. RUPESH stated he would text OWEN once RUPESH arrived. SYED also messaged RUPESH to "call Owen." This same date, RUPESH received $1,000 transfer from SYED, from a joint bank account held with an individual law enforcement believes is SYED's wife.

25. On April 29, 2024, RUPESH received an additional $1,000 payment from a bank account held by Fayez corporation, the account whose authorized signer was SYED's wife. WhatsApp communications recovered from RUPESH's phone (believed to be the

burner phone) reveal that during this timeframe, RUPESH communicated with an individual identified in his contact list as "JEFF," who is believed to be SYED. On this same date, the individual identified as "JEFF" messaged RUPESH "I am sending you 1000" consistent with the amount of money RUPESH received the same day from Fayez corporation. JEFF further messaged RUPESH that he should communicate with OWEN about booking a hotel. RUPESH messaged the individual believed to be OWEN identified by the contact "OW" asking if RUPESH should book a hotel in L.A. OWEN messaged RUPESH "Yea."

26. Various additional communications discovered on RUPESH's phone (believed to be the burner phone) provide further evidence that OWEN and "JEFF" (believed to be SYED) were coordinating the retrieval of fraudulent proceeds from various victims. On May 1, 2024, OWEN messaged RUPESH for the "Amount." RUPESH responded to OWEN "50K." OWEN instructed RUPESH "Go LA." "JEFF" also messaged RUPESH "Owen will give you 2000." RUPESH responded "You gave me 1000. Waiting on owen." Additionally, that same evening, OWEN messaged RUPESH with the address of Scottsdale Victim M.P. At approximately 9:18 pm, RUPESH messaged "JEFF" that he was "Going to Arizona state…"

27. On May 2, 2024, RUPESH and OWEN engaged in numerous phone and text communications. JEFF further messaged RUPESH asking for the total number of ounces. RUPESH responded to "JEFF" "1ozx46" which is the amount of gold obtained from Scottsdale victim M.P. Additionally, later that afternoon, OWEN messaged RUPESH the address of Marana, Arizona victim M.D. Shortly after, phone records reflect that SYED called RUPESH on his personal phone. They spoke for almost three minutes. They engaged in a second call a short time later for approximately 38 seconds. Further communications occurred between OWEN and JEFF to RUPESH that also appear to relate to coordinating the delivery from fraud victim M.D. The following day, May 3,

2023, the day after RUPESH's arrest, the phone evidence reveals that SYED attempted to call RUPESH multiple times on RUPESH's personal phone.

DEFENDANT SYED'S LINK TO OTHER FRAUD VICTIMS IN THE SCHEME:

28. SYED is also linked by additional evidence to other fraud victims and couriers in the scheme. Victim L.F. from Carmel, Indiana, lost approximately $48,000 in the scheme. On February 23, 2024, L.F. provided $48,000 cash to an individual she believed was a representative of the FTC. L.F. thought something was wrong and took a photo of the driver, who was on the phone. L.F. also photographed the driver's vehicle and license plate. The registered owner of this vehicle was the defendant SYED.

29. On March 21, 2024, courier Imran Shaikh was arrested in connection with another controlled delivery from Random Lake, Wisconsin victim S.S. Shaikh was arrested attempting to retrieve a package purporting to be cash from victim S.S. Shaikh was also later identified as the courier who retrieved $48,000 cash from Indiana victim L.F. on February 23, 2024. Phone records, evidence recovered from Shaikh's phone, and the photo taken of Shaikh holding his phone also establish that during the approximate time of retrieval of the package of cash from L.F., Shaikh communicated with SYED.

SYED'S STATEMENT TO LAW ENFORCEMENT, SEPTEMBER 2024

30. SYED generally denied any involvement in the scheme or the conspiracy. Relating to Shaikh (Imran), SYED claimed that Shaikh was SYED's cousin and that they communicated frequently. SYED further stated that on the day of the Wisconsin incident, Shaikh borrowed SYED's car for a job opportunity. SYED denied knowing why Shaikh was arrested and what he did. SYED claimed he found out later that it was for fraud. SYED claimed Shaikh was framed because he did not speak English. When questioned about why SYED was speaking with Shaikh relating to the Indiana victim pickup, SYED

stated that he spoke with his cousin Shaikh frequently. SYED further stated he did not recall why he was speaking with his cousin at that time.

31. SYED denied ever speaking with OWEN. SYED initially denied having his contact information on his phone. Later in the interview, SYED stated he received OWEN's number from Shaikh (Imran) in the last few months and that he had tried calling him but could not get through.

32. When questioned about his involvement with RUPESH, SYED stated he hired RUPESH for a job and gave him an advance and he suddenly disappeared. SYED stated that RUPESH never actually worked. SYED claimed he provided RUPESH $1000. SYED further stated he only spoke with RUPESH once or twice and that RUPESH was going to take orders for the gas stations and deliver them the next day. SYED further denied directing RUPESH to do pickups.

Events Leading to November 21, 2024 – Federal Arrest Warrant Served on Syed in the Chicago, Illinois Area:

33. On or about September 16, 2024, Magistrate Judge Maria Valdez from the Northern District of Illinois signed a federal search warrant authorizing a search of the gas station where Syed worked, located at 1331 N Farnsworth Ave, Aurora, Illinois. On or about the same, the Magistrate also signed a search warrant authorizing a search of SYED's person.

34. As indicated, on or about September 17, 2024, agents executed the federal search warrant. Additionally, SYED was arrested on State charges from Hamilton County, Indiana for conduct related to this investigation. During the execution of this warrant, agents recovered a cell phone believed to be SYED's personal phone, **Subject Phone 1**. While at the gas station that day, law enforcement interviewed an employee of the gas station ("Employee One"). Employee One said that SYED worked at the gas station since 2020. She further stated that SYED always carried two cell phones: an iPhone and an

Android phone. During the execution of the above warrant, law enforcement only recovered one phone from SYED, an iPhone. A review of this phone did not contain any incriminating messages. However, SYED's phone had the same WhatsApp contact number for the "OW" as RUPESH saved on SYED's phone as the "OW." As indicated above, various incriminating messages between RUPESH and SYED/JEFF and RUPESH and OWEN were recovered from RUPESH's phones. Additionally, incriminating videos were recovered on SYED's phone to include videos of packages that appear to be in SYED's vehicle and that also appear to relate to the fraud scheme under investigation. One of the videos recovered from SYED's phone from April 22, 2024, shows a package that appears to be in the front seat of SYED's vehicle. The package is wrapped and with handwriting addressed to "Alamadar Hamdani, Department of Justice 950 Pennsylvania Ave. Washington D.C. 20530."

35. As detailed above, use of electronic communications over the phones was a significant component of the fraud scheme under investigation. Fraudsters contacted victims by phone. SYED and other coconspirators communicated with one another by phone. Defendant's co-conspirator, RUPESH, who was interviewed by law enforcement on or about May 2, 2024 indicated that in relation to his pickup and delivery of gold, that he received a phone, and that he was directed to change phones frequently. After his arrest on or about May 2, 2024, RUPESH relayed to law enforcement that he had great concerns that information would also be deleted from the phones that had been used.

36. Prior to seeking the November 20, 2024 complaint and federal arrest warrants authorized by the U.S. Magistrate in this District, the FBI learned that, while on release in his State case, on or about November 4, 2024, RUPESH fled the country on an international flight after obtaining a new passport from India. In large part because of these circumstances, the government sought and obtained the federal arrest warrants for SYED and RUPESH from this District.

SYED'S FEDERAL ARREST – NOVEMBER 21, 2024:

37. On November 21, 2024, federal agents arrested SYED at the same gas station in Illinois previously searched on or about September 17, 2024. According to the arresting officers, before the November 21st arrest, SYED was standing behind the counter inside the gas station. The Subject Phones were found in proximity to SYED, in the area behind the counter where SYED had been standing. When asked who to call and inform about his arrest, SYED asked the agents to call his wife. Agents asked which phone was his, and SYED stated that **Subject Phone 3** was his and that **Subject Phone 2** was his wife's phone. When asked how to contact his wife if he had her phone, he responded that his wife had two phones. SYED then told agents to call his wife from **Subject Phone 2**, not **Subject Phone 3**. SYED gave agents the pin code to **Subject Phone 2** to allow them to find his wife's phone number since he did not have it memorized, but he did not provide a pin code for **Subject Phone 3**. The Subject Phones were recovered and taken into the custody of the FBI in Naperville, Illinois.

38. On November 27, 2024, a federal search warrant was obtained for **Subject Phone 2** and **Subject Phone 3** in the Northern District of Illinois.[5]

39. The Subject Phones were subsequently transported to the Federal Bureau of Investigation Phoenix, Arizona Division around December 2, 2024 because the complaint for the arrest of SYED originated out of the District of Arizona. After the Subject Phones were received in Arizona, the FBI requested that a Search Warrant be issued in the District of Arizona since the Subject Phones would be extracted/searched in the District

[5] The affidavit in support of those search warrants also inadvertently misstated that incriminating messages were recovered from Subject Phone 1, Syed's phone, when these messages were recovered from RUPESH's phones. Additionally, the affidavit attached and referenced the complaint that contained the inadvertent misstatements referenced in footnote 1 of this affidavit.

of Arizona. Therefore, the Illinois federal search warrant for **Subject Phone 2** and **Subject Phone 3** was not executed.

40. Based on my training and experience, and the facts above, I believe that both **Subject Phones** were in SYED's possession and were devices that SYED used to communicate with others, despite his claim that **Subject Phone 2** belonged to his wife.

41. Based on my training and experience, I know that cellular phones may contain relevant evidence of the Subject Offenses, including text messages made or received from co-conspirators as reflected by the messages already recovered from coconspirator RUPESH's phones in this case, and other incriminating evidence recovered in SYED's phone. Moreover, digital photographs located in the memory of the cell phones may also contain images, and additional evidence relating to the Subject Offenses.

42. In addition, based on my training and experience, I know that information stored within a cellular phone may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within a cell phone can indicate who has used or controlled the cell phone and/or the phones with whom the user is communicating.

43. Additionally, information stored within a cell phone may indicate the geographic location of the participants in criminal offenses at a particular time (*e.g.*, location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Stored electronic data may also provide relevant insight into the state of mind of individuals who are communicating with the cell phone user as it relates to the offense under investigation. For example, information in the cell phones may indicate motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting

communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by breaking the cell phone itself or by a program that deletes or over-writes the data contained within the cell phone, such data will remain stored within the cell phone indefinitely. Because in my experience and in the experience of other agents, defendants use telephones to contact co-conspirators, there is probable cause to believe that the phones seized in SYED's constructive possession, described further in Attachment A, contains evidence of the Subject Offenses.

SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

44. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored.

PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

45. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the phones described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

46. The review may include the following techniques (the following is a nonexclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in the phones to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

CONCLUSION

47. Based on the above information, I respectfully submit that there is probable cause to believe that violations of Title 18, United States Code, Section 1956 (Conspiracy to Commit Money Laundering) and Title 18, United States Code, Section 1349 (Conspiracy to Commit Wire Fraud) have been committed, and that evidence relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Phones**, as further described in Attachments A-1 and A-2.

48. I therefore respectfully request that this Court issue a search warrant for the phones, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

CAROL-ANNE DOWLING

Digitally signed by CAROL-ANNE DOWLING
Date: 2024.12.17 15:45:51 -07'00'

Carol-Anne Dowling, Special Agent
Federal Bureau of Investigation

Subscribed and Sworn to telephonically
on this 17th day of December, 2024

Lynnette C. Kimmins

LYNNETTE C. KIMMINS
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF ARIZONA

ATTACHMENT A-1

DESCRIPTION OF ITEMS TO BE SEARCHED

A white Apple iPhone in a red case seized during the arrest of Ahmed Maqbul Sayed on November 21, 2024, presently in the custody of the Federal Bureau of Investigation in Arizona. (Subject Phone #2)

ATTACHMENT A-2

DESCRIPTION OF ITEMS TO BE SEARCHED

A blue OnePlus Android phone in a blue case seized during the arrest of Ahmed Maqbul Sayed on November 21, 2024, presently in the custody of the Federal Bureau of Investigation in Arizona. (Subject Phone #3)

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence, instrumentalities, and contraband concerning violation of Title 18, United States Code, Sections 1349 and 1956 ("Subject Offenses") for the time-period of January 2023 to present as follows:

1. Financial information and wire/money transfers that appears tied to the fraudulent scheme described above, including banking information, Western Union, MoneyGram, RIA, Walmart, U.S. Postal Service, Federal Express, UPS (or any other mailing service), Green Dot, I-Tunes and any other bank and/or financial institution transactions, including all correspondence and communications pertaining to such transfers, account information, statements, invoices, transfers, receipts, senders/recipients, destination/return labels, U.S. currency, direct deposits, mobile deposits, checks (including electronic checks), and money orders;

2. All records and information associated with the use of crypto-currency including wallet addresses, seed phrases, transaction hashes, and receipts containing withdrawal, transfer, or deposit information.

3. All information pertaining to the impersonation of the U.S. Government or U.S. Government Agencies, including the Federal Bureau of Investigation (FBI), the Federal Trade Commission, the National Cyber Investigative Joint Task Force (NCIJTF), and the Internal Revenue Service (IRS) and Department of Justice.

4. All information pertaining to evidence of scams or frauds including Microsoft/computer hacking, and targeting elderly persons;

5. Records or information pertaining to proceeds of a fraud scheme/scam, including without limitation, United States and/or foreign currency, gold, cryptocurrency, documentation of financial transactions, bank statements, checks, books, records, invoices, payment receipts, money orders, cashier's checks, bank checks, credit card receipts, credit card statements, minute books, passwords and keys, and other items evidencing the obtaining, secreting, transferring, and/or concealment of assets and the obtaining, secreting, transferring, concealment, and/or expenditure of money as part of the Subject Offenses;

6. All information related to gold or cash as used in the fraud scheme, including the exchange of US currency for gold, the exchange of gold for US currency, and the delivery, transportation, and shipment information for gold or currency;

7. Lead and/or victim lists, or any other lists or descriptions identifying potential victims, subjects and co-conspirators, including contact information;

8. Victim or co-conspirator credit card and other financial information including but not limited to bills and payment records, bank accounts, bank records, financial account statements, receipts and other documentation or notations of financial information, checks, money orders, direct deposits, and all internet-related financial transactions;

9. Travel documents related to the fraud scheme, including but not limited to airline tickets, car rental agreements, commercial tickets, passports, and visas or any information pertaining to such travel.

10. Communications by coconspirators relating in any way to the crimes under investigation.

11. Communications relating to the coconspirators state of mind as it relates to the crimes under investigation.

12. This warrant further authorizes the forensic examination of the phones identified in Attachment A to secure the following additional evidence:

13. Evidence of who used, owned, or controlled the Subject Phones at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

14. Evidence indicating how and when the Subject Phones was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the Subject Phones' user(s);

15. Evidence indicating the Subject Phones' user or coconspirator's state of mind as it relates to the crimes under investigation;

16. Evidence of the attachment to the Subject Phones of other storage devices or similar containers for electronic evidence;

17. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Phones;

18. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Phones;

19. Records of or information about Internet Protocol addresses used by the Subject Phones;

20. Records of or information about the Subject Phones' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

21. All location history associated with the device including GPS system points, vehicle navigation, and any other location data during the Subject Offenses;

22. Call logs relating to communications concerning violations of the Subject Offenses;

23. Text, email, or chat messages (including any photos or media exchanged) concerning violations of the Subject Offenses;

24. Photos and/or videos relating to violations of the Subject Offenses.

During the execution of the search warrants for the Subject Phones, law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of the subject Ahmed Syed ("SYED"), to the fingerprint scanner of the device; or (2) hold a device in front of SYED's face to activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

ADDENDUM TO ATTACHMENT B

The government's review of electronic storage media, including cell phones, already in its possession shall be conducted pursuant to the following protocol:

The government must make reasonable efforts to use methods and procedures that will locate those categories of data, files, documents, or other electronically stored information that are identified in the warrant, while minimizing exposure or examination of categories that will not reveal the items to be seized in Attachment B.

The review of electronically stored information and electronic storage media described in Attachment A may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures if those procedures are designed to minimize the review of information not within the list of items to be seized as set forth in Attachment B:

a. examination of categories of data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;

c. surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word or concept searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B; and

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment B.

Law enforcement personnel are not authorized to conduct additional searches for any information beyond the scope of the items to be seized by this warrant as set forth in Attachment B. To the extent that evidence of crimes not within the scope of this warrant appears in plain view during the government's review, the government shall submit a new search warrant application seeking authority to expand the scope of the search prior to searching portions of that data or other item that is not within the scope of the warrant. However, the government may continue its search of that same data or other item if it also contains evidence of crimes within the scope of this warrant.